ROCHESTON® CERTIFIED CYBERSECURITY ENGINEER

Certified by Rocheston®

RCCE® Certification Program Guide

ROCHESTON
NEW YORK
DISTINGUISHED

About Rocheston

Rocheston, a young New York based internet technology start-up, despite being in its nascent stage, is a company that is raring to go. Rocheston has a worldwide presence, with its headquarters in New York. The company's technology development center is based out of Chennai, with reach offices in Singapore and Dubai.

The team at Rocheston consists of young, liberal, innovative and forward-thinking individuals **who want to make a difference and change the world. At its core, Rocheston is a next-generation innovation company**, with cutting-edge research and development in emerging technologies such as Cybersecurity, Internet of Things, Big Data and automation.

Rocheston Certified Cybersecurity Engineer (RCCE®)

The RCCE Level 2 program will give you a detailed, in-depth knowledge and hands-on labs. You will have mastery over hacking technologies and tools. **The Level 2 program covers advanced futuristic hacking stuff.** For instance, it looks at advanced blockchain exploits, quantum computing and cryptography, advanced ransomware and cryptojacking, etc.

The RCCE® Level 1 is a mandatory requirement, to move to the Level 2 program.

ROCHESTON®

Target Audience

There is a growing need for an equally sophisticated cybersecurity framework with the increased dependence on interconnected cloud technologies.

Individuals who wish to build a career in cybersecurity across the following industries:

- Healthcare
- Smart Cities
- Industry 4.0
- Transportation
- Electronics
- Governance
- Automation
- Robotics
- Telecom
- Smart Appliances
- Department of Defense
- Finance

Eligibility

A Bachelor's degree with one year of professional experience or credential in computer science, engineering, mathematics, or other information technology related fields. You will need basic hacking, networking, system administration, and Linux skills.

What the course will consist of:

- A 5-day Training Program
- Time: 9:30 AM – 6 PM
- The provision of an active web portal
- Seminars conducted by qualified engineers
- Best in-class environment

Cost

For pricing in your region, please contact the local distributor.

Note: If you don't have basic hacking skills you can attend Rocheston's Extreme Hacking Level 1 Program (which is included in this course).

ROCHESTON®

RCCE® Exam

- Exam can be taken on Rocheston Cyberclass or Pearson VUE testing platform.
- Multiple Choice Objective Questions
- Total count - approximately 90 questions for each exam
- Pass Percentage: 72%
- Retake Policy - You may retake the exam any time on an additional fee. For further details contact the exam coordinator.

The Cyberclass Web Portal

The access to an online e-learning platform will be given to attendants on registration. It will contain a series of study videos, pre-recorded lectures, white papers, educational animations and power point presentations. The Web Portal can be used to catch-up on a missed session or to view an attended session again.

http://cyberclass.rocheston.com

ROCHESTON®

Course Completion

- On completing the course and successfully passing the exam, the candidate will be provided with a RCCE certification.
- Candidates are free to use the logo as per the Terms & Conditions as a Rocheston Certified Professional.
- The candidate will also receive a Welcome Kit and login information to access the Members' Portal.
- The Members' Portal is an online forum for Certified RCCEs to interact.
- The certification is valid for two years and it can be renewed online.
- Contact the course coordinator for any enquiries about the renewal fee or downloading of the updated course material.

Course Objectives

In the RCCE® Level 2 program you will learn to:

- Utilize sophisticated and extremely advanced phishing techniques.
- Carry out advanced blockchain exploits, cryptocurrency mining attacks and cyberweapon attacks.
- Understand quantum computing and advanced cloud security.
- Complement RCCE Level 1, RCCE Level 2 imparts specialist knowledge on persistent privacy problems, IoT vulnerabilities,open source intelligence, sophisticated stealth tools in the Dark web and other specialist concepts.
- Understand the types of cryptography and its history, encryption, data protection, key generation algorithms, RSA security and cryptography.
- Mail authentication tokens, authorization, and implementation of private servers.

13 15

Course Outline

RCCE® Level 2

Module 1: Sophisticated and Extremely Advanced Phishing Techniques Harvested by Chinese and Russian Hackers

Module 2: Deep Network Insights for Deeper Analytics

Module 3: Read Privileged Kernel Memory and Leak Data to Escalate Privileges

Module 4: Advanced Blockchain Exploits and Cryptocurrency Mining Attacks

Module 5: Sophisticated Government use of Cyberweapon Attacks and How they work

Module 6: Principles of Quantum Entanglement to Secure Communication (Unhackable networks)

Module 7: Guidance For Cybersecurity Disclosure and Advanced Techniques for Cyber Bounty hunting

Module 8: Advanced Mobile Banking and ATM Trojans

Module 9: Quantum Computing and Cryptography

Module 10: Dark Web and How to Download Sophisticated Stealth Tools

Module 11: Advanced Cloud Security - Azure, AWS, Digital Ocean, Google VM.

Module 12: H2O Driverless AI, Amazon SageMaker, and Azure Machine Learning AutoML

Module 13: Deepfakes and Generating Automated Fake news

Module 14: Advanced Threat Modelling Attacks

Module 15: Cognitive-Powered Security Intelligence Platform

Module 16: Advanced Ransomware and Cryptojacking Attacks

Module 17: Open Source Intelligence in Cybersecurity

Module 18: Attacking AI Chatbot and Voice Assistants - Siri, Google Home and Alexa

Module 19: DeepLocker: How AI Can Power a Stealthy New Breed of Malware

Module 20: Cybersecurity Insurance

Module 21: Advanced File System Protection With Cyber Deception

Module 22: Legal AI: How Machine Learning Is Aiding, Concerning Law Practitioners

Module 23: Advanced Threat Hunting Techniques

Module 24: Vulnerability Management Process Based on Weaponization and Asset Value

Module 25: Passwordless Authentication With FIDO

Module 26: Advanced PowerShell Attacks

Module 27: Next Generation of the Cyber Range Attacks

Module 28: Advanced Payment Gateway and Financial Cyberattacks

Module 29: Developing Immersive Cybersecurity Simulation

Module 30: Advanced DDOS Attacks Using IoT Botnets

Module 31: Attacking Hidden Endpoint Management Firewalls and IDS

Module 32: Advanced BGP Router Attacks

Module 33: Machine Learning with Automated Software Vulnerabilities

Module 34: Hacking Medical IoT Devices

Module 35: Hacking Biometric Security, and Facial Recognition Systems

Module 36: Threat Intelligence Models for Cyber Warfare

Module 37: Artificial Intelligence and Cyberwarfare

Module 38: Hacking Connected Cars

Module 39: Hacking Power Grids

Module 40: Advanced Mobile Phone Hacking, Spying, GPS and Monitoring

Module 41: Home Automation and IoT Gadgets

Module 42: How To Use Tensorflow

Module 43: Advanced EMP Cyberattacks

Module 44: Hacking heart devices, pacemakers, insertable cardiac

Module 45: Integrating IoT Security into Vulnerability Management Program

Module 46: Containers & Cloud Native Security

ROCHESTON

https://www.facebook.com/Rocheston/

https://www.linkedin.com/company/rocheston-accreditation-institute/

https://twitter.com/rocheston